JD:GK
F. #2019R00850

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER THE SEARCH OF THE ELECTRONIC DEVICE KNOWN AND DESCRIBED AS: ONE BLACK LG ARISTO 3+ WITH IMEI 355292100548043	**TO BE FILED UNDER SEAL** APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 19-1019 M

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR WARRANT TO SEARCH AND SEIZE

I, KEVIN TAGNOSKY, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of an electronic device currently in law enforcement custody, more particularly described in Attachment A and the extraction from that device of electronically stored information described in Attachment B.

1. I have been a Detective with the New York City Police Department ("NYPD") for more than 6 years, and for the past 3 years I have been designated a Task Force Officer with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"). I am currently assigned to the Joint Firearms Task Force, where I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for firearms-related investigations. I have participated in investigations involving search

warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit come from my personal observations, my training and experience, information obtained from other agents and witnesses and information from law enforcement and public records databases. The statements described in this affidavit are set forth in sum, substance, and in part.

IDENTIFICATION OF THE PROPERTY TO BE SEARCHED

3. The property to be searched is one Black LG Aristo 3+ with IMEI 355292100548043 (the "DEVICE"). The DEVICE is currently in the lawful possession of the ATF in the Eastern District of New York.

4. The applied-for warrant would authorize the forensic examination of the DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that MECHEAL LESLIE, also known as "Michael Leslie," committed violations of federal criminal law, to wit, together with others, not being a licensed importer, licensed manufacturer or licensed dealer of firearms, did knowingly and willfully engage in the business of dealing in firearms, and in the course of such business did

ship, transport and receive one or more firearms in interstate and foreign commerce, in violation of Title 18, United States Code, Section 922(a)(1)(A)) (the "Subject Offense"). There is also probable cause to search the DEVICE described in Attachment A for evidence, instrumentalities, contraband and/or fruits of this crime, further described in Attachment B.

6. On October 8, 2019, the Honorable Peggy Kuo, United States Magistrate Judge in the Eastern District of New York, signed a complaint and affidavit in support of an application for an arrest warrant and a search warrant of the defendant MECHAEL LESLIE's residence, located at 165-20 115th Avenue in Jamaica, New York (the "Premises") (hereinafter, "Search Warrant 1"). (19-MJ-909). A copy of the executed arrest warrant, search warrant, and affidavit in support thereof are attached hereto as Exhibit A. The contents of Exhibit A are hereby fully incorporated herein.

7. Search Warrant 1, among other things, permitted law enforcement agents to seize cellphones and other electronic devices found within the Premises and to search them for evidence of the Subject Offense.

8. Law enforcement agents executed Search Warrant 1 and effectuated the defendant MECHEAL LESLIE's arrest on October 9, 2019. Among other items, law enforcement agents seized and searched a cell phone and a computer from within the Premises.

9. Upon a review of electronically stored information on the cell phone seized pursuant to Search Warrant 1, the cell phone was found to contain evidence of the Subject Offense. For example, the search revealed, among other things, an extended online chat conversation between the defendant MECHAEL LESLIE and another individual discussing

the acquisition and sale of firearms.

10. In addition to the cell phone seized from within the Premises, law enforcement agents also identified and seized the DEVICE, a second cell phone which was found in the defendant MECHAEL LESLIE's pocket. At the time that the DEVICE was located, LESLIE was standing in the outdoor area directly in front of his residence; therefore, the DEVICE was not within the Premises at the time of its seizure incident to LESLIE's arrest. The DEVICE is currently in the lawful possession of the ATF in the Eastern District of New York.

11. Based on my training and experience, I know that individuals that traffic in firearms commonly use mobile devices such as cellular telephones to communicate with co-conspirators and customers through voice calls, text messages and other means. In addition, the facts set forth herein indicate that the defendant MECHAEL LESLIE has used at least one other cellular telephone to communicate with individuals regarding firearms sales.

12. For the reasons stated above and further described in Exhibit A, I submit that there is probable cause that the DEVICE contains evidence of the Subject Offense.

TECHNICAL TERMS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless

telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a

handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. Based on my training, experience and research, I know that the DEVICE has capabilities that allow them to serve as a web browser, email client, Internet messaging device, telephone, digital camera, portable media player, GPS navigation device, and PDA.

In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

15. Based on my knowledge, training and experience, I know that those who are engaged in conspiracies often communicate with co-conspirators to plan and execute crimes by means of wireless telephone (including by means of text messages, electronic mail and social media messages), and record the contact information of criminal associates in the "contacts" section of such telephones. Those who commit such offenses may retain evidence of their participation in such offenses on wireless telephones through call records, text messages, WhatsApp messages, Facebook messages, Instagram messages, emails or photos. That data (including communications and photographs) may also constitute evidence of their association with criminal organizations, conspiracies and/or enterprise. Moreover, information stored on such telephone, including photographs, emails and text messages, can be used to help identify the users of such telephones.

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. There is probable cause to believe that things that were once stored on the DEVICE may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they

have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes

ATTACHMENT B

1. Text messages, emails, instant messages and messages sent through telephone applications—including, but not limited to, Facebook Messenger and WhatsApp—on the Device described in Attachment A (collectively, "communications") that relate to or concern violations of Title 18, United States Code, Sections 922 and 924 (firearms offenses) and Title 21, United States Code, Section 841 (drug trafficking) by SHARIF LUCAS and others, dated in or about and between May 3, 2019, and September 3, 2019, including the following:

   a. Communications with customers related to the sale of controlled substances;

   b. Communications related to sources of supply of controlled substances;

   c. Communications related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

   d. Communications relating to types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions; and

   e. Communications with "Tyriq LNU."

2. Information from the DEVICE's contacts relating to any interlocutors in the communications described in Paragraph 1.

3. Evidence of user attribution, dated in or about and between May 3, 2019, and September 3, 2019, showing who used or owned the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, browsing history and records of Internet Protocol addresses used.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to communicate with coconspirators regarding an agreement to unlawfully distribute controlled substances, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICE consistent with the warrant. The examination may require authorities to employ techniques,

including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

21. I submit that this affidavit supports probable cause for a search warrant authorizing law enforcement to search the DEVICE described in Attachment A and to conduct a forensic examination for the purpose of identifying the electronically stored information described in Attachment B.

REQUEST FOR SEALING

22. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into criminal organizations and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem

appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Kevin Tagnosky
Task Force Officer
Joint Firearm Task Force
ATF

Subscribed and sworn to before me
on October 31, 2019:

THE HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Description of the Property to Be Searched

The property to be searched is one Black LG Aristo 3+ with IMEI 355292100548043 (the "DEVICE"). The DEVICE is currently in the Eastern District of New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Description of the Things to Be Seized

1. All records and information on the device described in Attachment A that relate to violations of Title 18 United States Code Section 922(a)(1)(A) (the "SUBJECT OFFENSE"), involving MECHEAL LESLIE and occurring after May 1, 2018, including:

a. lists of, and/or contact information for, individuals with whom MECHEAL LESLIE discussed the SUBJECT OFFENSE, including planning and coordinating the SUBJECT OFFENSE, and related identifying information;

b. Any communications regarding the SUBJECT OFFENSE, or the planning thereof;

c. any information related to the SUBJECT OFFENSE (including names, addresses, phone numbers, or any other identifying information of individuals);

d. photographs, video, text messages, instant messages and all other electronic communications, saved audio files, web browsing history and other records regarding the SUBJECT OFFENSE;

e. records of or information about the DEVICE's Internet activity regarding the SUBJECT OFFENSE, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

f. statements and other information regarding the SUBJECT OFFENSE.

2. Evidence of user attribution showing who used or owned the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, self-identifying information and photographs, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Exhibit A

JD:GK
F. #2019R00850

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ARREST WARRANT FOR MECHEAL LESLIE AND FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS 165-20 115TH AVENUE, JAMAICA, NEW YORK, AND ANY LOCKED OR ENCLOSED CONTAINERS THEREIN	**TO BE FILED UNDER SEAL** COMPLAINT AND AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR AN ARREST WARRANT AND A SEARCH WARRANT (18 U.S.C. § 922(a)(1)(A)) **19-MJ-909**

AFFIDAVIT IN SUPPORT OF AN ARREST WARRANT AND AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

KEVIN TAGNOSKY, being duly sworn, deposes and states that he is a Detective with the New York City Police Department ("NYPD"), designated as a Task Force Officer with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") Joint Firearms Task Force, duly appointed according to law and acting as such.

Between in or about May 2018 and March 2019, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant MECHEAL LESLIE, also known as "Michael Leslie," together with others, not being licensed importers, licensed manufacturers or licensed dealers of firearms, did knowingly and willfully engage in the business of dealing in firearms, and in the course of such business did ship, transport and receive one or more firearms in interstate and foreign commerce.

(Title 18, United States Code, Section 922(a)(1)(A))

I. Introduction

A. Affiant

1. I have been a Detective with the NYPD for more than 6 years, and for the past 3 years I have been designated a Task Force Officer with the ATF. I am currently assigned to the Joint Firearms Task Force, where I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for firearms-related investigations. I have participated in investigations involving search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. I have personally participated in the investigation of the offenses discussed below.

2. I make this Affidavit in support of an application for an arrest warrant for MECHEAL LESLIE, also known as "Michael Leslie," for violations of 18 United States Code Section 922(a)(1)(A) and for an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below (the "SUBJECT PREMISES"), further described in Attachment A, for the items and information described in Attachment B. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI").[1] Because this

[1] "Electronically Stored Information" or "ESI" includes, consistent with Federal Rule of Criminal Procedure 41 and the Advisory Committee Comments to the 2009 amendments, writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained, including

affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Premises

3. The SUBJECT PREMISES is the northern residential unit within a blue, two-story building located at 165-20 115th Avenue Jamaica, New York 11434 which contains two separate residential units, each accessible through separate front doors on 166th street. The SUBJECT PREMISES is accessible through a front door on the right-hand side of the building when viewed from 166th Street, as well as through a back entrance. A wood sign outside the SUBJECT PREMISES displays "165-20" in black lettering beneath a large window on the right-hand side of the house as viewed from 166th Street. Photographs of the outside of the dwelling are included in Attachment A.

4. This warrant application does not seek permission to enter the southern residential unit within the building located at 165-20 115th Avenue Jamaica, New York 11434, which is accessible through a front door on the left-hand side of the building when viewed from 166th Street.

5. Law enforcement agents have conducted physical surveillance and searches of public records in an attempt to determine whether any shared spaces—such as basements or attics—are accessible to both residential units. Because the building located at 165-20 115th

---

all types of computer-based information as may be developed over time. "Computer data" as used herein is synonymous with ESI.

Avenue Jamaica, New York 11434 was converted from a single-unit dwelling to a two-unit dwelling, law enforcement agents have been unable to confirm the existence of any such spaces. However, if any such spaces exist, I submit that those spaces should be considered part of the SUBJECT PREMISES for the purposes of this application, and there is probable cause to enter those spaces for the reasons stated herein.

C. The Subject Offenses

6. For the reasons detailed below, I submit that there is probable cause to believe that MECHEAL LESLIE, also known as "Michael Leslie," has committed violations of Title 18, United States Code, Section 922(a)(1)(A) (illegal firearms trafficking), and that the Subject Premises contains evidence, fruits, and instrumentalities of such violations.

II. Probable Cause Regarding Subject's Commission of the Subject Offenses

7. Since at least March 2019, the ATF and NYPD (together, "the investigative agencies") have been investigating a series of firearms sales that occurred in or otherwise affected the Eastern District of New York in May and June, 2018. The investigation concerns possible violations of Title 18, United States Code, Sections 922(a)(1)(A) and 2 (the "Subject Offenses"), among other crimes.

8. On or about March 11, 2019, the Royal Barbados Police Force (the "RBPF") notified U.S. law enforcement investigators that they had intercepted and seized a package shipped from Queens, New York to Barbados via DHL after an inspection revealed that its contents included a microwave containing three firearms and several hundred rounds of ammunition ("Package A"). The firearms included (1) one Smith & Wesson .40 caliber pistol with serial number FZV3416; (2) one Smith & Wesson .40 caliber pistol with serial number PBN6673; and (3) one Taurus .357 caliber revolver with serial number NJ81824.

The ammunition consisted of 433 rounds of ammunition of various calibers, including calibers .40, .357, and .38. The listed sender of the package was "Jimmy Rogers," 56 Rochester Ave, Brooklyn, NY 11233, with phone number (516) 444-1824. The listed consignee was "Omar Rogers," with phone number (246) 838-2379.

9. The RBPF further notified U.S. law enforcement investigators that the DHL delivery driver who delivered Package A had previously flagged consignee "Omar Rogers" as suspicious in December 2018. In particular, in 2018, the DHL delivery driver reported to his supervisor that "Omar Rogers" provided only a telephone number and had no listed address, and when contacted by telephone, "Omar Rogers" had asked the DHL delivery driver to meet him at an uninhabited residence to receive the shipment. The DHL delivery driver further reported that "Omar Rogers" had received a shipment of a microwave in Barbados in a similar manner on at least one prior occasion.

10. Law enforcement investigators also determined that a package with the same listed consignee phone number as Package A, (246) 838-2379, was seized in the United States on June 4, 2018, after U.S. law enforcement agents found two firearms concealed in a speaker box ("Package B"). Package B was dropped off and processed on May 17, 2018. The listed sender of Package B was "Jamal Parris," with phone number (516) 590-4035. The listed recipient of Package B was "Randy Parris."

11. Through database searches, law enforcement investigators determined that the listed phone number for the sender of Package B, (516) 590-4035, is associated with MECHEAL LESLIE. In addition, the phone number (516) 590-4035 was also

identified as a number used by MECHEAL LESLIE in a domestic violence investigation report dated on or about February 26, 2018.

12. Through a social media search, law enforcement investigators determined that the phone number listed for the recipients of Packages A and B, (246) 838-2379, is associated with a Facebook account whose user is connected as a current "friend" of Facebook user "Mecheal Tie Leslie."

13. Law enforcement investigators obtained video surveillance from the facilities from which Packages A and B were shipped during the times when the packages were dropped off and processed. A review of the surveillance footage confirms that Packages A and B were both shipped by the same individual. The video surveillance footage for both shipments shows the individual filling out forms, dropping off the packages that were later determined to contain firearms, and paying for shipment.

14. Law enforcement agents have since identified the individual who shipped Packages A and B to be MECHEAL LESLIE based on a comparison of the video surveillance footage captured during both shipments with photographs of LESLIE contained on his New York City identification card and on social media websites, as well as the investigators' direct observation of LESLIE while conducting surveillance of him at the SUBJECT PREMISES.

III. Probable Cause to Search and Seize

15. A search of law enforcement databases shows that the SUBJECT PREMISES is listed as the current residence of MECHEAL LESLIE. A law enforcement database search further reveals that the SUBJECT PREMISES was the reported location of two

separate domestic violence complaints involving LESLIE and his girlfriend[2], and that LESLIE previously reported to the NYPD that he resided at the SUBJECT PREMISES.

16. I have conducted surveillance of the SUBJECT PREMISES over the course of several weeks and have observed both MECHEAL LESLIE and his girlfriend enter and exit the SUBJECT PREMISES, through the front door, on multiple occasions, including as recently as yesterday, October 7, 2019.

17. Law enforcement agents have confirmed through real estate and real property websites that the SUBJECT PREMISES contains two entirely separate residential units, each accessible through a separate front door, and that MECHAEL LESLIE occupies the northern unit, accessible by a door that appears on the right-hand side of the building when viewed from 166th Street. Law enforcement personnel executing the search will not enter the southern unit connected to the SUBJECT PREMISES and will make reasonable efforts to search only the portion of the SUBJECT PREMISES actually occupied or utilized by LESLIE. Law enforcement personnel executing the search will not search portions of the Subject Premises that appear to be occupied by residents other than LESLIE, or seize items that appear to belong to residents of the Subject Premises other than LESLIE.

18. Based on my training and experience, I am aware that individuals engaged in illegal firearms trafficking often store firearms, ammunition, and other gun paraphernalia, as well as packaging material and items used to conceal firearms, in their places of residence.

[2] The identity of MECHEAL LESLIE's girlfriend is known to law enforcement and has been confirmed through a review of law enforcement databases and recent posts on LESLIE's girlfriend's social media accounts.

19. Based on my training and experience, I am also aware that individuals who transport firearms by mail often keep communications and records regarding their firearms shipments on computers, cellphones and other electronic devices, which they often store in their homes. Accordingly, and as discussed more fully below, I submit that there is probable cause to seize computers and other electronic devices that were instrumentalities of the Subject Offenses, and to search for evidence of the Subject Offenses on those electronic devices.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

20. As described above and in Attachment B, this application seeks permission to search for records that might be found in the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a cellphone, a computer's hard drive or other storage media.[3] Thus, the search warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. *Probable cause.* I submit that if a computer or storage medium is found in the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after

[3] Based on my training and experience, I use the following technical terms storage media to mean: any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. As discussed above, based on my training and experience, I believe that computer equipment was used to generate, store, and print documents used in the postage meter scheme. Based on the surveillance of CHE, there is reason to believe that there is a computer system currently located in the Subject Premises that was used to create counterfeit postage labels.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can

record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such

information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw

conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

23. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 21, United States Code, Sections 853(a) and 853(p))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS TWO AND THREE

6. The United States hereby gives notice to the defendant that, upon his conviction of either of the offenses charged in Counts Two and Three, the government will seek forfeiture in accordance with Title 18, United States Code, Section 924(d)(1) and Title 28, United States Code, Section 2461(c), which require the forfeiture of any firearm or ammunition involved in or used in any knowing violation of Title 18, United States Code, Section 922 or Section 924, including but not limited to the Bryco Arms .22 caliber semi-automatic pistol with serial number 1090345 recovered from the defendant in Brooklyn, New York, on or about September 2, 2019.

7. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(c) has been placed beyond the jurisdiction of the court;

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

25. Because several people might share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. Law enforcement personnel executing the search will make reasonable efforts to identify and search only electronic devices used to commit violations of 18 U.S.C. §§ 922(a)(1)(A) based on the location of the electronic devices within the SUBJECT PREMISES as well as conversations with individuals present at the SUBJECT PREMISES. If electronic devices identified through such means and seized during the execution of a search warrant are determined to belong to an innocent third party, the investigative agencies will release the device as soon as the device has been imaged and has been confirmed to be "clean," i.e., does not contain any contraband or evidence of a crime.

26. Electronic devices seized pursuant to this warrant may include cellphones. In my training and experience, users of cellphones that offer the ability to unlock by fingerprint or facial recognition often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. If a user has enabled his or her cellphone to be unlocked by either fingerprint or facial recognition, he or she can unlock the device by raising the cellphone to his or her face, or tapping the screen.

27. The passcodes or passwords that would unlock cellphones seized pursuant to this search warrant are not known to law enforcement. Thus, it will likely be necessary to press the fingers of the user of the cellphones to the device's fingerprint sensor, or hold the cellphones in front of the user's face to activate the facial recognition sensor, in an attempt to unlock the devices for the purpose of executing the search authorized by this warrant. Attempting to unlock the cellphones via fingerprint, or via facial recognition by holding the device in front of the user's face, is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

28. I also know from my training and experience that cellphone devices that can access the internet typically will have a feature that allows a user to erase the contents of the device remotely. logging into the Internet, the user or any other individual who possesses the user's account information can take steps to completely wipe the contents of the device, thereby destroying evidence of criminal conduct, along with any other information on the device. The only means to prevent this action is to disable the device's ability to connect to the Internet immediately upon seizure, which requires either access to the device itself to

alter the settings, or the use of specialized equipment that is not consistently available to law enforcement agents at every arrest.

29. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of MECHEAL LESLIE to the fingerprint sensor of the any cellular telephones reasonably believed to be used by LESLIE, or hold such devices in front of LESLIE's face (and, if necessary, hold LESLIE in place while holding the Subject Devices in front of his face), for the purpose of attempting to unlock the device via fingerprint or facial recognition in order to search the contents as authorized by this warrant.

A. Review of ESI

1. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information falling within the categories set forth in Attachment B.

2. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a

cursory examination of each document in a file cabinet to determine its relevance);

- "scanning" storage areas for deliberately hidden files and to discover and possibly recover recently deleted data;
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation;[4] and;
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or electronically stored information of a nature described in Attachment A.

3. In conducting the search authorized by the Search Warrant, the government shall make reasonable efforts to restrict its search to files, documents or other electronically stored falling within the categories of evidence specified in Attachment B. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

B. Return of ESI

4. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the

[4] Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure that is not captured by a keyword search because the information does not contain the keywords being searched.

offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion

5. Based on the foregoing, I respectfully request the court to issue a warrant to arrest MECHEAL LESLIE for violations of Title 18 United States Code Section 922(a)(1)(A), and a warrant to search the SUBJECT PREMISES and to seize the items and information specified in Attachment B to this affidavit and to the Search and Seizure Warrant.

WHEREFORE, your deponent respectfully requests that the defendant MECHEAL LESLIE be dealt with according to law.

I further request that the Court order that all papers in support of this Application, including the Affidavit, the Arrest Warrant, and Search Warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the target of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation by

allowing the target to flee before he can be arrested and the search of the Subject Premises can be conducted.

KEVIN TAGNOSKY
Task Force Officer
Joint Firearm Task Force
ATF

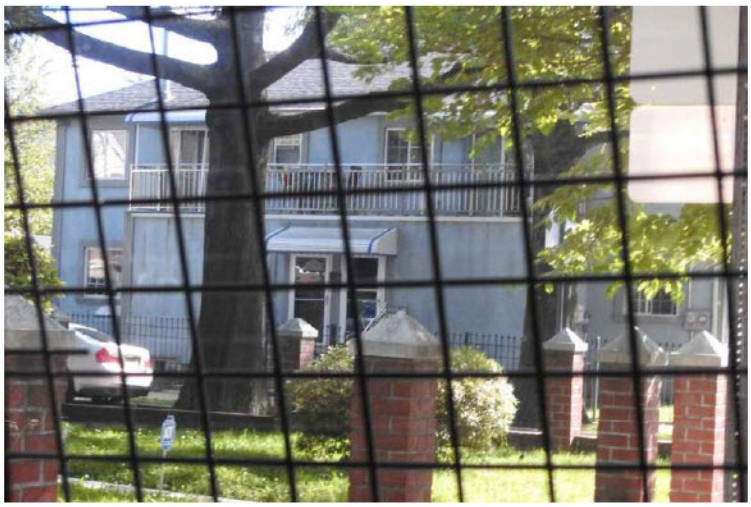
Sworn to before me by
telephone on this 8th day of
October, 2019

HONORABLE PEGGY KUO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

1. The SUBJECT PREMISES is the northern residential unit within a blue, two-story building located at 165-20 115th Avenue Jamaica, New York 11434 which contains two separate residential units, each accessible through separate front doors on 166th street. The SUBJECT PREMISES is accessible through a front door on the right-hand side of the building when viewed from 166th Street, as well as through a back entrance. A wood sign outside the SUBJECT PREMISES displays "165-20" in black lettering beneath a large window on the right-hand side of the house as viewed from 166th Street. Photographs of the outside of the dwelling, viewed from 166th Street and 115th Avenue, respectively, appear below.




15 Av

ATTACHMENT B
Property to be Seized

I. Items to be Seized: Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the SUBJECT PREMISES, INCLUDING ANY LOCKED AND CLOSED CONTAINERS, AND CLOSED ITEMS CONTAINED THEREIN, include the following evidence, fruits, and/or instrumentalities of violations of Title 18 United States Code Section 922(a)(1)(A) (illegal firearms trafficking):

1. Firearms, ammunition, other weapons, bullet proof vests, gun leather and related items;

2. All evidence concerning payment for firearms, including without limitation, currency or proceeds of firearms trafficking, controlled substances of any kind, and mixtures and substances suspected to contain a detectable amount of controlled substances;

3. All items of clothing consistent with the clothing worn by MECHEAL LESLIE in video surveillance footage captured within shipment facilities in May 2018 and March 2019, including but not limited to a gray/green zip-up hooded sweatshirt or jacket, a black winter hat, and a gray and white patterned zip-up sweatshirt;

4. All evidence reasonably consistent with the concealment of firearms, including but not limited to large electronic devices that have been partially disassembled or deconstructed;

5. All records and information relating to violations of Title 18 United States Code Section 922(a)(1)(A), involving MECHEAL LESLIE and occurring after May 1, 2018, including:

   a. Records, receipts, invoices, or account statements related to the sale, billing, and payment for firearms;

b. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs and electronic messages establishing possession, access to, transportation, or shipment of firearms through interstate or foreign commerce, including by United States mail, common carrier or DHL; and

c. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transportation of firearms through interstate or foreign commerce, including by United States mail, common carrier or DHL; and

d. Computers or storage media used as a means to commit the violations described above.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of MECHEAL LESLIE onto the fingerprint sensor of any cellphones reasonably believed to be used by LESLIE, or hold such cellphones in front of LESLIE's face to activate the facial recognition sensor (and, if necessary, hold LESLIE in place while holding the cellphones in front of his face), in order to gain access to the contents of the cellphones as authorized by this warrant.

II. Search and Seizure of Electronically Stored Information

The items to be seized from the SUBJECT PREMISES include any computer devices, storage media, and related electronic equipment that may contain or constitute fruits, evidence, and/or instrumentalities of the Subject Offenses falling within the categories set forth in

Section I above. In addition to seizing any such computer devices, storage media, and related electronic equipment, this warrant also authorizes their copying for later review.

To facilitate this review, the items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any records or other items which evidence ownership, control, or use of, or access to any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to sales receipts, warranties, bills for internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

Any materials seized under this Section that are later determined not to contain or constitute fruits, evidence, and/or instrumentalities of the Subject Offenses falling within the categories set forth in Section I above will be returned to the SUBJECT PREMISES or to persons reasonably believed to have rightful ownership or custody of the devices.

Review of ESI

Following seizure and/or copying of any computer devices, storage media, and related electronic equipment, law enforcement personnel (which may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to Attachment B-I above.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section I of this Attachment. However, law enforcement personnel are authorized to conduct

a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

For purposes of this Attachment B, computer devices, storage media, and related electronic equipment includes any computer, computer system and high-speed data processing device, including but not limited to desktop computers, notebook computers, tablets, and server computers; tapes; cassettes; cartridges; streaming tape; commercial software and hardware; network hardware and software; computer disks; disk drives; monitors; computer printers; modems; tape drives; disk application programs; data disks; system disk operating systems; tape systems and hard drive and other computer related operation equipment; routers, modems, and network equipment used to connect to the Internet; cameras; video cameras; scanners; computer photographs; graphic interchange formats and/or photographs; undeveloped photographic film, slides, and other visual depictions of such graphic interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG); any electronic data storage devices including, but not limited to hardware, software, diskettes, magnetic media floppy disks; backup tapes, CD-ROMS, DVD, RAM, flash memory devices, and other storage mediums; and any input/output peripheral devices, including but not limited to data security devices.

AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

United States of America
v.
MECHEAL LESLIE, also known as "Michael Leslie,"

Case No. 19-MJ-909

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) MECHEAL LESLIE, also known as "Michael Leslie,",

who is accused of an offense or violation based on the following document filed with the court:

❒ Indictment ❒ Superseding Indictment ❒ Information ❒ Superseding Information ☑ Complaint

❒ Probation Violation Petition ❒ Supervised Release Violation Petition ❒ Violation Notice ❒ Order of the Court

This offense is briefly described as follows:

Together with others, not being licensed importers, licensed manufacturers or licensed dealers of firearms, knowingly and willfully engaging in the business of dealing in firearms, and in the course of such business shipping, transporting and receiving one or more firearms in interstate and foreign commerce, in violation of Title 18, United States Code, Section 922(a)(1)(A).

Date: 10/08/2019

Issuing officer's signature

City and state: Brooklyn, New York

Hon. Peggy Kuo, U.S.M.J.
Printed name and title

Return

This warrant was received on *(date)* _____, and the person was arrested on *(date)* _____
at *(city and state)* _____.

Date: _____

Arresting officer's signature

Printed name and title

This second page contains personal identifiers provided for law-enforcement use only and therefore should not be filed in court with the executed warrant unless under seal.

(Not for Public Disclosure)

Name of defendant/offender: _____

Known aliases: _____

Last known residence: _____

Prior addresses to which defendant/offender may still have ties: _____

Last known employment: _____

Last known telephone numbers: _____

Place of birth: _____

Date of birth: _____

Social Security number: _____

Height: _____ Weight: _____

Sex: _____ Race: _____

Hair: _____ Eyes: _____

Scars, tattoos, other distinguishing marks: _____

History of violence, weapons, drug use: _____

Known family, friends, and other associates *(name, relation, address, phone number)*: _____

FBI number: _____

Complete description of auto: _____

Investigative agency and address: _____

Name and telephone numbers (office and cell) of pretrial services or probation officer *(if applicable)*: _____

Date of last contact with pretrial services or probation officer *(if applicable)*: _____

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* THE PREMISES KNOWN AND DESCRIBED AS 165-20 115TH AVENUE, JAMAICA, NEW YORK, AND ANY LOCKED OR ENCLOSED CONTAINERS THEREIN	)	Case No. 19-MJ-909

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of New York *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before October 22, 2019 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: October 8, 2019 3:46 pm

Judge's signature

City and state: Brooklyn, New York

Hon. Peggy Kuo U.S.M.J.

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 19-MJ-909	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

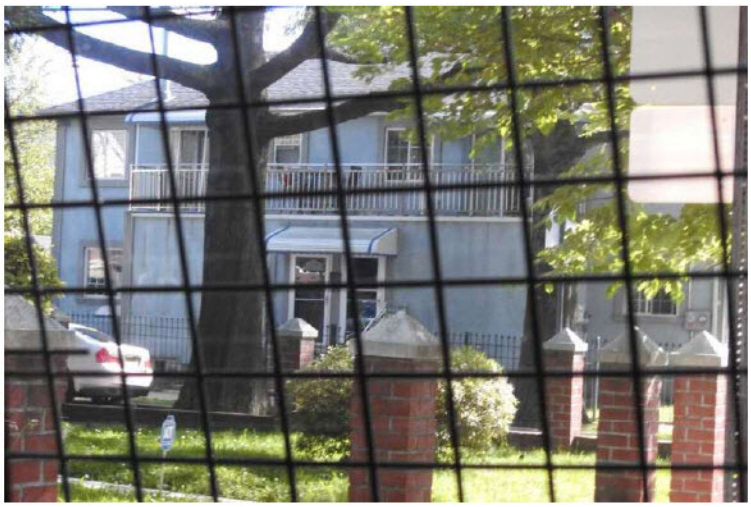
_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

1. The SUBJECT PREMISES is the northern residential unit within a blue, two-story building located at 165-20 115th Avenue Jamaica, New York 11434 which contains two separate residential units, each accessible through separate front doors on 166th street. The SUBJECT PREMISES is accessible through a front door on the right-hand side of the building when viewed from 166th Street, as well as through a back entrance. A wood sign outside the SUBJECT PREMISES displays "165-20" in black lettering beneath a large window on the right-hand side of the house as viewed from 166th Street. Photographs of the outside of the dwelling, viewed from 166th Street and 115th Avenue, respectively, appear below.




15 Av

ATTACHMENT B
Property to be Seized

I. Items to be Seized: Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the SUBJECT PREMISES, INCLUDING ANY LOCKED AND CLOSED CONTAINERS, AND CLOSED ITEMS CONTAINED THEREIN, include the following evidence, fruits, and/or instrumentalities of violations of Title 18 United States Code Section 922(a)(1)(A) (illegal firearms trafficking):

1. Firearms, ammunition, other weapons, bullet proof vests, gun leather and related items;

2. All evidence concerning payment for firearms, including without limitation, currency or proceeds of firearms trafficking, controlled substances of any kind, and mixtures and substances suspected to contain a detectable amount of controlled substances;

3. All items of clothing consistent with the clothing worn by MECHEAL LESLIE in video surveillance footage captured within shipment facilities in May 2018 and March 2019, including but not limited to a gray/green zip-up hooded sweatshirt or jacket, a black winter hat, and a gray and white patterned zip-up sweatshirt;

4. All evidence reasonably consistent with the concealment of firearms, including but not limited to large electronic devices that have been partially disassembled or deconstructed;

5. All records and information relating to violations of Title 18 United States Code Section 922(a)(1)(A), involving MECHEAL LESLIE and occurring after May 1, 2018, including:

   a. Records, receipts, invoices, or account statements related to the sale, billing, and payment for firearms;

b. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs and electronic messages establishing possession, access to, transportation, or shipment of firearms through interstate or foreign commerce, including by United States mail, common carrier or DHL; and

c. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transportation of firearms through interstate or foreign commerce, including by United States mail, common carrier or DHL; and

d. Computers or storage media used as a means to commit the violations described above.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of MECHEAL LESLIE onto the fingerprint sensor of any cellphones reasonably believed to be used by LESLIE, or hold such cellphones in front of LESLIE's face to activate the facial recognition sensor (and, if necessary, hold LESLIE in place while holding the cellphones in front of his face), in order to gain access to the contents of the cellphones as authorized by this warrant.

II. Search and Seizure of Electronically Stored Information

The items to be seized from the SUBJECT PREMISES include any computer devices, storage media, and related electronic equipment that may contain or constitute fruits, evidence, and/or instrumentalities of the Subject Offenses falling within the categories set forth in

Section I above. In addition to seizing any such computer devices, storage media, and related electronic equipment, this warrant also authorizes their copying for later review.

To facilitate this review, the items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any records or other items which evidence ownership, control, or use of, or access to any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to sales receipts, warranties, bills for internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

Any materials seized under this Section that are later determined not to contain or constitute fruits, evidence, and/or instrumentalities of the Subject Offenses falling within the categories set forth in Section I above will be returned to the SUBJECT PREMISES or to persons reasonably believed to have rightful ownership or custody of the devices.

Review of ESI

Following seizure and/or copying of any computer devices, storage media, and related electronic equipment, law enforcement personnel (which may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to Attachment B-I above.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section I of this Attachment. However, law enforcement personnel are authorized to conduct

a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

For purposes of this Attachment B, computer devices, storage media, and related electronic equipment includes any computer, computer system and high-speed data processing device, including but not limited to desktop computers, notebook computers, tablets, and server computers; tapes; cassettes; cartridges; streaming tape; commercial software and hardware; network hardware and software; computer disks; disk drives; monitors; computer printers; modems; tape drives; disk application programs; data disks; system disk operating systems; tape systems and hard drive and other computer related operation equipment; routers, modems, and network equipment used to connect to the Internet; cameras; video cameras; scanners; computer photographs; graphic interchange formats and/or photographs; undeveloped photographic film, slides, and other visual depictions of such graphic interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG); any electronic data storage devices including, but not limited to hardware, software, diskettes, magnetic media floppy disks; backup tapes, CD-ROMS, DVD, RAM, flash memory devices, and other storage mediums; and any input/output peripheral devices, including but not limited to data security devices.